Communication Plan

CloudShield

March 8th, 2025

Table of Contents

1. Communication Tools

In order to meet the deliverables of this project, team CloudShield will be using the following tools:

- Discord: this free-source platform was chosen by the team because it allows us to easily communicate, interact and share insights about the project. All of the group meetings will be held through this platform;

- Google Drive: this is a cloud-based storage that was shared between the team members to better organize all of the file projects;

2. Meeting Schedules

The team decided to establish a strict schedule in order to be able to deliver the requirements for this project. The schedule is as follows:

Meeting Schedule		
March 6th	18h30 - 21h30	Discord
March 7th	18h30 - 21h30	Discord
March 8th	17h00 - 20h00	Discord
March 9th	17h00 - 20h00	Discord
March 10th	18h30 - 21h30	Discord
March 11th	18h30 - 21h30	Discord
March 12th	18h30 - 21h30	Discord
March 13th	Presentation	

CloudShield

2

3. Team Roles

The team also established a role for each of the members, in order to maintain an organized and well structured plan. The following table shows the roles designated to each team member:

Team Roles	Responsibility
Team Leader	Alex
Communications	Gonçalo
Report	Tatiana
Presentation	Tiago
Note Taker	Frederico

4. Response Times

It is important to organize all of the tasks, as well as prioritize those which are urgent. To better classify and differentiate the urgent tasks from the non-urgent ones, we set up a template in order to do so:

Response Time		
Urgent	8h	ex: Help request
Non-urgent	12h	ex: Informational, status update
Template		
Urgency: Urgent/Non-urgent		
Topic (Task that is related to + subject)		
Brief explanation and/or status update		

5. Progress Tracking System

In order for all of the team members to keep track of each other's progress, we decided to use the Google Docs, Spreadsheet.

Function	Description/Goal	Expected time	Date limit	Completed	Responsable
Conflit & Communition docs	Define and conclude Conflict resolution and Communication plans	1h	03/06/25	☐	All of us ▾
Create private subnet				☐	Tiago ▾
Deploy Win server & hardening	accessible only via vpn tunneling, encrypt data at rest and transit, deploy sysmon			☐	Tiago ▾
Deploy Linux server & hardening	Create a sample file with PII and PCI, data encrypted at rest and transit			☐	Gonçalo ▾
SIEM	Choose 1 and justify why, make it analyse on real time,			☐	Frederico ▾
Python script	simulate attack that must trigger siem with a script in python with a new library			☐	Frederico ▾
Cloud monitoring	demonstrate how the attack TTPs would be detected in the AWS Cloud using VPC Flow Logs and any additional automation necessary			☐	Tatiana ▾
AWS Lambda	function triggering a relevant response to a detected threat			☐	Tatiana ▾
Monitoring	Monitor for threat activity and Monitor Security Logs for failed SSH attempts			☐	Tatiana ▾
				☐	▾
				☐	▾
				☐	▾
				☐	▾
				☐	▾
				☐	▾
				☐	▾
				☐	▾
				☐	▾
				☐	▾
				☐	▾
				☐	▾

CloudShield